CLAIMS

What is claimed is:

1. A memory architecture, comprising:

   a) an unprotected memory space configured to store encrypted information, said encrypted information corresponding to a plain text version thereof;

   b) a first protected memory space configured to store at least a subset of operating system instructions; and

   c) a second protected memory space configured to store said plain text version of said encrypted information;

wherein said operating system instructions in said first protected memory space operate on said plain text version of said encrypted information in said second protected memory space.

2. The memory architecture of Claim 1, wherein said encrypted information comprises an instruction to load said encrypted information from said unprotected memory space into said first protected memory space.

3. The memory architecture of Claim 2, further comprising one or more instructions to decrypt said encrypted information in said first protected memory space to form said plain text version.

4. The memory architecture of Claim 1, wherein said encrypted information comprises an instruction to store at least one of (i) said encrypted information in said first protected memory space, (ii) said plain text version in said first protected memory space, and (iii) said plain text version in said second protected memory space.

5. The memory architecture of Claim 1, wherein said unprotected memory space is further configured to store executable code and data.

6. The memory architecture of Claim 1, wherein said subset of operating system instructions comprises at least one member selected from the group consisting of:

a) fetching or pre-fetching at least part of said executable code and data;

b) interpreting at least part of said executable code and data;

c) translating at least part of said executable code and data; and

d) determining whether information in said unprotected memory space comprises encrypted information.

7. The memory architecture of Claim 6, further comprising a third protected memory configured to store said plain text version after at least one operating system instruction has operated thereon.

8. The memory architecture of Claim 1, further including an authorization key or message digest corresponding to or associated with said encrypted information.

9. The memory architecture of Claim 8, wherein said first protected memory space further comprises a table or list linking said authorization key or message digest to said plain text version in said second protected memory space.

10. The memory architecture of Claim 9, wherein said table comprises a non-zero location of said plain text version in said second protected memory space.

11. The memory architecture of Claim 1, wherein said first protected memory space further comprises a table or list linking a unique identifier for said encrypted information to a

pointer for at least one of (i) a location of said plain text version and (ii) a location of a decryption tool for decrypting said encrypted information.

12. A system for operating on encrypted information, comprising:

a processor; and

a memory architecture of comprising:

an unprotected memory space configured to store encrypted information, said encrypted information corresponding to a plain text version thereof;

a first protected memory space configured to store at least a subset of operating system instructions; and

a second protected memory space configured to store said plain text version of said encrypted information, wherein said operating system instructions in said first protected memory space operate on said plain text version of said encrypted information in said second protected memory space;

wherein said processor is configured to execute said operating system instructions.

13. The system of Claim 12, wherein said unprotected memory space comprises at least part of a hard disk.

14. The system of Claim 12, wherein said first protected memory space comprises at least part of a first ROM.

15. The system of Claim 12, wherein said second protected memory space comprises at least part of a second ROM.

16. The system of Claim 12, further comprising at least one peripheral device configured to operate in accordance with said encrypted information.

17. A method of operating on encrypted and/or hidden information, comprising the steps of:

a) transferring said encrypted and/or hidden information to a first protected memory address inaccessible to a user-accessible software program, but accessible to an operating system instruction set;

b) if said encrypted and/or hidden information comprises encrypted information, decrypting said encrypted information to form a decrypted version of said encrypted information; and

c) storing said first protected memory address in a second protected memory address inaccessible to a user-accessible software program, but accessible to an operating system instruction set, wherein said second protected memory address is linked to an original location of said encrypted and/or hidden information.

18. The method of Claim 17, wherein said encrypted and/or hidden information comprises encrypted information.

19. The method of Claim 18, wherein said original location of said encrypted information is in unprotected memory.

20. The method of Claim 18, further comprising linking a decryption key to at least one of said encrypted information, said original location and said first protected memory address.

21. The method of Claim 17, further comprising operating on said decrypted version and/or hidden information entirely within protected memory.

22. A medium or waveform containing a computer-readable set of instructions adapted to perform the method of Claim 17.

23. A system for hiding information, comprising:

a) one or more units of information to be hidden;

b) a unique identifier for each of said units of information;

c) one or more tools configured to hide each of the units of information at a known location in protected memory; and

d) a second location in protected memory adapted to store each of said unique identifiers and a corresponding known location in protected memory where the corresponding unit of information is hidden.